



Security Manager's Guide for

DOD E-Business Exchange System

Version 3.0

May 2000

Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 400
Newport News, Virginia 23602

SMG for DEBX Version 3.0

The following trademarks and registered trademarks are mentioned in this document. Within the text of this document, the appropriate symbol for a trademark (™) or a registered trademark (®) appears after the first occurrence of each item.

HP is a registered trademark of Hewlett-Packard Company, and HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

UNIX is a registered trademark of The Open Group.

Copyright © 2000
Inter-National Research Institute, Inc.
All Rights Reserved

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (NOV 1995).

Security Manager's Guide for DEBX

Contents

Section 1	Introduction	1-1
1.1	Menu Bar Functions	1-2
1.2	Documentation Conventions	1-3
Section 2	System Menu	2-1
2.1	Set Menu Font	2-2
2.2	System Exit	2-3
Section 3	Security Menu	3-1
3.1	Audit Status	3-2
3.2	Audit Log	3-4
3.3	Security Alert Log	3-6
3.4	Archive Logs	3-9
Section 4	Accounts Menu	4-1
4.1	View System Accounts	4-2
4.2	View User Accounts	4-4
4.3	View Roles	4-10
4.4	Archive Accts & Roles	4-18
4.5	Restore Accts & Roles	4-19
Section 5	Help	5-1
Index	Index-1	

List of Figures

Figure 2.1-1	SET MENU FONT Window	2-2
Figure 3.1-1	AUDIT STATUS Window	3-2
Figure 3.2-1	SECURITY AUDIT LOG Window	3-4
Figure 3.3-1	SECURITY ALERTS LOG Window	3-6
Figure 3.4-1	ARCHIVE LOGS Window	3-9
Figure 4.1-1	SYSTEM ACCOUNTS Window	4-2
Figure 4.2-1	USER ACCOUNTS Window	4-4
Figure 4.2-2	EDIT ACCOUNT Window	4-7
Figure 4.3-1	USER ROLES Window	4-11
Figure 4.3-2	ADD ROLE Window	4-12
Figure 4.3-3	EDIT ROLE Window	4-14
Figure 4.3-4	EDIT PERMISSIONS Window	4-16
Figure 4.4-1	ARCHIVE ACCTS & ROLES Window	4-18
Figure 4.5-1	RESTORE ACCTS & ROLES Window	4-19

List of Tables

Table 4.3-1	Security Administration Functions	4-15
Table 4.3-2	System Administration Functions	4-15

Section 1

Introduction

This guide provides information about security administration of the DOD E-Business Exchange System (DEBX), which is a Computer Software Configuration Item (CSCI) of the system identified as Electronic Commerce/Electronic Data Interchange (EC/EDI). The security manager, or a user assigned a security administration role, performs tasks such as maintaining audit logs and user accounts.

Each of the menus available from the main menu bar is presented as a section of this guide, as follows:

System Menu

Describes how to set the menu font size for the security application and to exit the system. ([Section 2](#))

Security Menu

Describes how to update audit status, review audit information, and archive audit logs. ([Section 3](#))

Accounts Menu

Describes how to view system accounts and to create, edit, archive, and restore user accounts and roles. ([Section 4](#))

Help

Describes the Help menu options, which enable you to view the online Help and documentation for DEBX. ([Section 5](#))

1.1 Menu Bar Functions

In addition to the menus described in [Section 1](#), the following function is provided through the main menu bar.

Role Box

The role box, beside the **Help** menu, displays the name of the role that is currently in use. If assigned to more than one role, you may also use this box to move between roles. To do so: Click the role box and select the desired role from the menu that appears. For additional information on roles, see [Section 4](#).

NOTE: The menus that appear on the main menu bar vary with each selected role. This guide discusses the menus and options available when the **SSO Default** role is selected. For information regarding the menus and options available for the other roles, see the DEBX Help system and the *System Administrator's Guide for DOD E-Business Exchange System*.

1.2 Documentation Conventions

The following text styles and formats are used throughout this manual to enhance readability:

- Text that you should enter from the keyboard (usually at a command prompt) or that appears on the screen as computer output is offset in `Courier` font. Examples are:

In the **Console** window, enter `/usr/sbin/sam` to run the HP System Administration Manager (SAM) and press **[Enter]**.

Log in as `secman`.

- **Helvetica** font is used to distinguish menu options, windows, buttons, and other text that appears on the screen (except for output that appears as a result of entering a command). Display text is spelled and punctuated exactly as it appears on the screen. Examples are:

From the **Security** menu, select **Audit Log**. The **SECURITY AUDIT LOG** window appears.

Click **APPLY** to save the changes or **CANCEL** to discard them.

- Field names within a window are displayed in **bold HELVETICA**. A brief description of the field follows immediately below. Examples are:

ACCT GROUP

Account group associated with the role.

CLASSIFICATION

Security classification of the role.

- Keyboard keys such as **[Enter]** and **[Tab]** are used within brackets and are also in **helvetica**.
- *Italicized letters* are used for emphasis.
- Commands should be entered as they appear with the following exceptions:
 - Within the body of a paragraph a command may be called out using quotation marks (e.g., use the “`ls`” command). Unless specified otherwise, do not enter the quotation marks when entering a command.
 - Generic or sample data within a command or screen output is offset in angle brackets (e.g., `setenv DISPLAY <local host>:0.0`). You should enter your specific information *without* the angle brackets in the command line.

- When a command is too long to fit on one line, every attempt will be made to break the line before you should enter a space. Unless noted otherwise, you should enter the command as one line with no space after the line break. Example:

```
Enter: echo "00 23 * * * su - ecpn -c /h/EC/progs/  
export_msg_list.sh > /dev/null 2>&1" >> /tmp/cron_root
```

Note that the command should be entered on one line with no returns and that there is no space between `progs/export_msg_list.sh`.

- If a command contains mutually exclusive options, the options are enclosed in brackets and separated by a vertical bar. For example:

```
dial [\m(local-prefix) | \m(long-dist-prefix)]
```

You should enter only one of the options *without* the brackets or vertical bar.

- Notes, cautions, and other critical information are contained in text boxes. For example:

NOTE: If you click **RESTORE**, the system overwrites the current account and role information on the workstation with the information on the tape.

- Sections of documentation that have changed since the last release of the DEBX documentation are denoted by a vertical bar in the outer edge of a page, adjacent to the modified text.
- Page numbering reflects the number of each page within a major section. For example, page 3-19 is the 19th page of Section 3.0. Figure numbering is also sequential; thus Figure 3.1-4 is the fourth figure in Section 3.1.
- Figures are designed to resemble on-screen graphics as closely as possible. Figure dimensions do not necessarily match the dimensions of actual menus and windows. All figures depicting windows contain *sample* data and should be used for reference purposes only.

Section 2

System Menu

The System menu provides the following options:

Set Menu Font

To set the font size for menus within the security application. ([Section 2.1](#))

System Exit

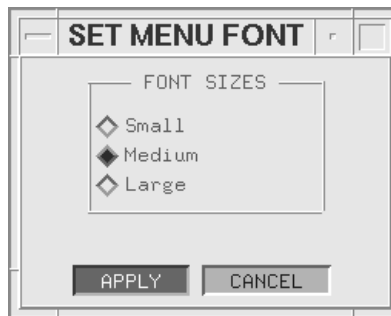
To exit the security application. ([Section 2.2](#))

2.1 Set Menu Font

Use the Set Menu Font option to set the font size for the menus within the security application.

1. From the **System** menu, select **Set Menu Font**. The **SET MENU FONT** window appears.

Figure 2.1-1 SET MENU FONT Window



2. Select the **Small**, **Medium**, or **Large** option button.
3. To save the change and close the window, click **APPLY**.
4. Select **System Exit** from the **System** menu and restart the security application for the change to take effect.

2.2 System Exit

Use the **System Exit** option to close all windows, exit the security application, and return to the login prompt.

This page has been intentionally left blank.

Section 3

Security Menu

The options on the **Security** menu enable you to maintain and view the audit and alert logs for each workstation on the LAN that is running DEBX. You must set the audit status options for each workstation individually.

The **Security** menu provides the following options:

Audit Status

To specify the type of information and level of detail that should be monitored for each workstation and to view current logs to determine if they should be archived or purged. ([Section 3.1](#))

Audit Log

To list audit events that occurred since the log was last purged. ([Section 3.2](#))

Security Alert Log

To list events generated by the security application since the log was last purged. ([Section 3.3](#))

Archive Logs

To archive alert and audit logs to tape. ([Section 3.4](#))

3.1 Audit Status

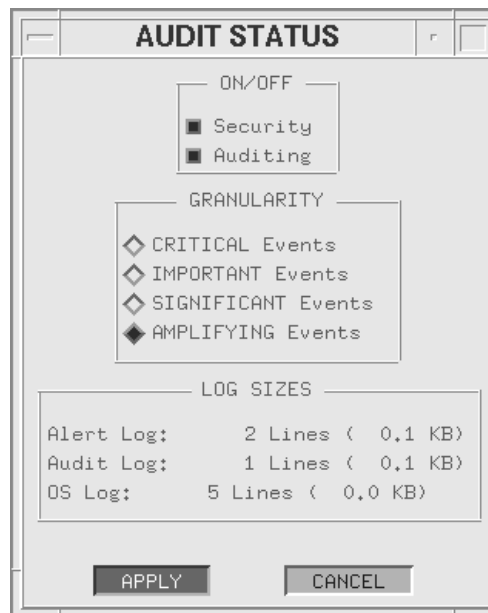
The Audit Status option enables you to turn the security and auditing functions on or off. When the security function alone is activated, the system records only the alerts that are generated by the applications running on the workstation. (For more information on the security alert log, see [Section 3.3](#).) If the auditing function is activated, the system also records the audit events that are generated by the applications running on the workstation. (For more information on the audit log, see [Section 3.2](#).) The type of information that is recorded in these logs depends on the level of detail that you have specified. Using the Audit Status option, you can do the following:

- [Activate](#) or deactivate the security and auditing functions.
- [Specify](#) the level of detail for the security logs.
- [View](#) the current size of the logs to determine if they should be archived or purged.

To activate or deactivate the security and auditing functions

1. From the Security menu, select Audit Status. The AUDIT STATUS window appears.

Figure 3.1-1 AUDIT STATUS Window



2. In the ON/OFF box, select the Security and Auditing check boxes to activate or deactivate them.
 - If Auditing is selected: The Security check box is also selected by default. Audit events and alerts are logged. Note that you *cannot* select the Auditing check box alone.
 - If Security alone is selected: Only alerts are logged.

Each application running on the workstation determines which events from that application will be logged. When an event is assigned both an audit command and an alert command:

- The event will be written in both logs if both Security and Auditing are selected.
- The event will be written *only* in the SECURITY ALERT LOG if Security is selected and Auditing is not selected.

To specify the level of detail for security logs

CRITICAL Events

Logging in and out; updating, exporting, or archiving user accounts or roles; archiving and purging logs; changing the audit status; and changing the security classification.

IMPORTANT Events

All CRITICAL events plus user entry or exit of classified functions.

SIGNIFICANT Events

All IMPORTANT events (and, therefore, all CRITICAL events) plus printing or archiving data.

AMPLIFYING Events

All of the above plus all of the information that applications installed on the workstation are designed to collect, such as modifying data in window fields.

To view the current log sizes

The LOG SIZES box indicates the current size of each log in number of lines (each line representing one event) and in kilobytes. Log sizes are updated as audit records are added. Use the information in this box to determine when logs should be archived and purged.

Click APPLY to save changes in the AUDIT STATUS window or CANCEL to discard them. Clicking either button closes the window.

3.2 Audit Log

Each workstation running DEBX generates an audit log. Each log lists audit events generated by applications running on that machine since the log was last purged. Note that events are logged only if the **Security** and the **Auditing** check boxes are selected in the **AUDIT STATUS** window (described in [Section 3.1](#)).

Because each application determines which events are logged, a comprehensive list of entries for this window is not provided in this section.

Using the **Audit Log** option, you can do the following:

- [View](#) the audit log entries.
- [Print](#) a log.
- [Archive](#) audit information to a tape.
- [Purge](#) audit information from the log.

To view the audit log entries

From the **Security** menu, select **Audit Log**. The **SECURITY AUDIT LOG** window appears.

Figure 3.2-1 SECURITY AUDIT LOG Window

SECURITY AUDIT LOG

DTG	W/S	USER	GRAN LEVEL	APP	STATUS	AUDIT EVENT	
301754:37Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SSO Default
301751:25Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to ECPN Default
311749:42Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SA Default
311549:18Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SSO Default
311549:04Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SA Default
311547:45Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SSO Default
311541:49Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to ECPN Default
311519:27Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SA Default
311511:31Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to ECPN Default
311508:17Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SSO Default
311452:46Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SSO Default
311448:10Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to ECPN Default
311441:52Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SA Default
311250:47Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to ECPN Default
311245:04Z	AUG 98	larry	ecpn	SIGNIFICANT	MELog	SUCCESS	Changing Role to SA Default

PRINT

ARCHIVE

PURGE

EXIT

The SECURITY AUDIT LOG window displays an entry under the following column headings for each audit entry in the log. Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

DTG

Date-time group when the audit event occurred.

W/S

Name of the workstation where the audit event occurred.

USER

User at the time of the audit event.

GRAN LEVEL

Granularity of the audit event. (Described in [Section 3.1.](#))

APP

Application that generated the audit event.

AUDIT EVENT

Description of the audit event.

To print a log

In the SECURITY AUDIT LOG window, click PRINT to generate a printed report of the window's contents. A detailed description of how to set up a printer is available in the *System Administrator's Guide for DOD E-Business Exchange System*.

To archive audit information to tape

In the SECURITY AUDIT LOG window, click ARCHIVE. The ARCHIVE LOGS window ([Figure 3.4-1](#)) appears. See [Section 3.4](#) for a description of this window.

To purge audit information from the log

In the SECURITY AUDIT LOG window, click PURGE. A confirmation window appears asking if you want to archive before purging. Archiving a log before purging is *strongly* recommended.

- If you select YES in the confirmation window, the ARCHIVE LOGS window ([Figure 3.4-1](#)) appears. See [Section 3.4](#) for instructions on archiving logs.
- If you select NO in the confirmation window, another confirmation window appears, asking if you are sure you want to purge the log. Select YES to purge or NO to stop the purge.

3.3 Security Alert Log

Each workstation running DEBX generates a security alerts log. This log lists the alerts generated by the security applications running on the workstation since the log was last purged.

Alerts will be logged only if the **Security** check box is selected in the **AUDIT STATUS** window (as described in [Section 3.1](#)). Because each application determines which alerts are logged, a comprehensive list of entries for this window is not provided in this section.

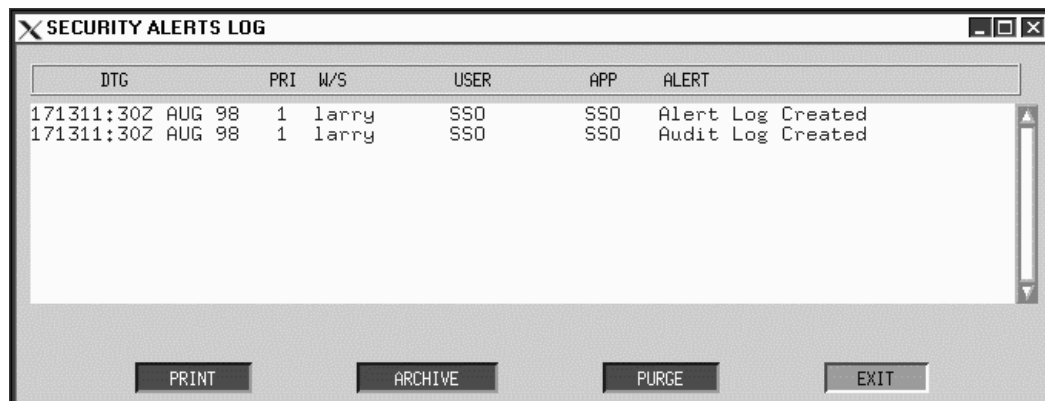
Using the **Security Alert Log** option, you can do the following:

- [View](#) the security alert log entries.
- [Print](#) a log.
- [Archive](#) security alert information to a tape.
- [Purge](#) security alert information from the log.

To view the security alert log entries

From the **Security** menu, select **Security Alert Log**. The **SECURITY ALERTS LOG** window appears.

Figure 3.3-1 SECURITY ALERTS LOG Window



The SECURITY ALERTS LOG window displays an entry under the following column headings for each alert entry in the log. Click on a column heading to sort the list by that heading. The default sort is the date-time group, listing the most recent record first.

DTG

Date-time group when the security alert occurred.

PRI

Priority of the security alert.

W/S

Name of the workstation where the security alert occurred.

USER

User at the time of the security alert.

APP

Application that generated the security alert.

ALERT

Description of the security alert.

To print a log

In the SECURITY ALERTS LOG window, click PRINT to generate a printed report of the window's contents. A detailed description of how to set up a printer is available in the *System Administrator's Guide for DOD E-Business Exchange System*.

To archive audit information to tape

In the SECURITY ALERTS LOG window, click ARCHIVE. The ARCHIVE LOGS window ([Figure 3.4-1](#)) appears. See [Section 3.4](#) for a description of this window.

To purge audit information from the log

In the SECURITY ALERTS LOG window, click PURGE. A confirmation window appears, asking if you want to archive before purging. Archiving a log before purging is *strongly* recommended.

- If you select YES in the confirmation window, the ARCHIVE LOGS window ([Figure 3.4-1](#)) appears. See [Section 3.4](#) for instructions on archiving logs.
- If you select NO in the confirmation window, another confirmation window appears, asking if you are sure you want to purge the log. Select YES to purge or NO to stop the purge.

3.4 Archive Logs

The Archive Logs option enables you to save the security alert and audit logs to tape.

To archive logs

1. From the Security menu, select Archive Logs. The ARCHIVE LOGS window appears.

Figure 3.4-1 ARCHIVE LOGS Window



2. Select any combination of logs to be archived. Note that a zero-sized log file cannot be archived, and it will not be listed as an option in this window.
3. Insert a tape and click ARCHIVE.
4. Click OK in the confirmation window to verify that the archive tape is ready for writing. A second confirmation window appears before proceeding with the archive process.
5. Click YES to continue with the archive, or NO to cancel the process.

NOTE: The archive process cannot be canceled after YES is selected.

This page has been intentionally left blank.

Section 4

Accounts Menu

The Accounts menu provides the following options:

View System Accounts

To view a list of all system accounts provided with the security application. System accounts *cannot* be modified by the security manager. ([Section 4.1](#))

View User Accounts

To create, edit, view, and maintain user accounts. ([Section 4.2](#))

View Roles

To view, create, or modify a role. ([Section 4.3](#))

Archive Accts & Roles

To archive accounts and roles to tape. ([Section 4.4](#))

Restore Accts & Roles

To restore accounts and roles to the workstation from tape. ([Section 4.5](#))

4.1 View System Accounts

The View System Accounts option enables you to view a database of all system accounts provided with the security application. System accounts include accounts that are required by the operating system. The list of accounts may vary, depending on the hardware platform running the security application.

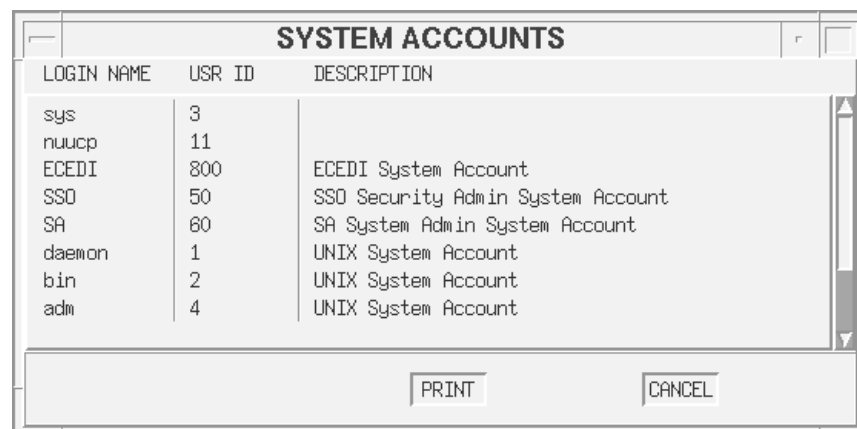
Using the View System Accounts option, you can do the following:

- [View](#) the system accounts database.
- [Generate](#) a printed report.

To view the system accounts database

From the Accounts menu, select View System Accounts. The SYSTEM ACCOUNTS window appears.

Figure 4.1-1 SYSTEM ACCOUNTS Window



LOGIN NAME	USR ID	DESCRIPTION
sys	3	
nuucp	11	
ECEDI	800	ECEDI System Account
SSD	50	SSD Security Admin System Account
SA	60	SA System Admin System Account
daemon	1	UNIX System Account
bin	2	UNIX System Account
adm	4	UNIX System Account

The data in the SYSTEM ACCOUNTS window is provided for information purposes only and cannot be modified. The window provides an entry under the following column headings for each system account in the database:

LOGIN NAME

Login name assigned to the account.

USR ID

Number assigned to the user by the system.

DESCRIPTION

Description of the account.

To generate a printed report

In the SYSTEM ACCOUNTS window, click PRINT. For a detailed description of how to set up a printer, see the *System Administrator's Guide for DOD E-Business Exchange System*.

4.2 View User Accounts

The View User Accounts option enables you to create, edit, view, and maintain user accounts. The accounts include default accounts and accounts added by any user that is assigned a security administrator role.

Three default user accounts are provided with the security application:

- *root* – privileged user account for the workstation; allows unrestricted access to all UNIX® system files.
- *secman* – security manager user account.
- *sysadmin* – system administration user account.

These default accounts are protected system files and cannot be edited or deleted.

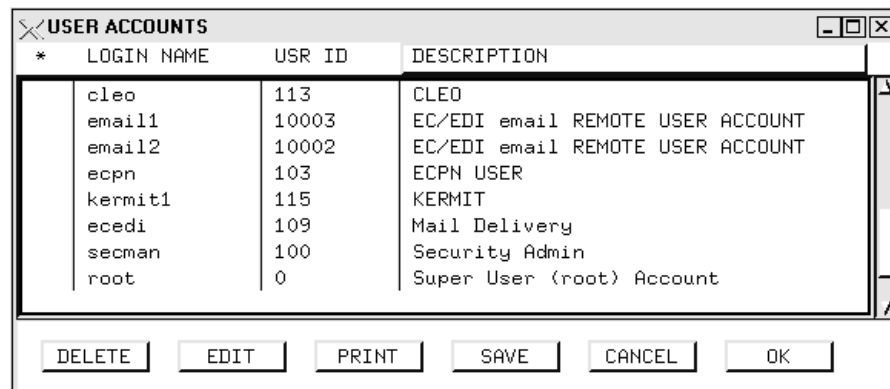
Using the View User Accounts option, you can do the following:

- [Access](#) the user accounts database.
- [Create](#) a user account.
- [Delete](#) a user account.
- [Retain](#) a user account marked for deletion.
- [Generate](#) a printed report.

To access the user accounts database

From the Accounts menu, select View User Accounts. The USER ACCOUNTS window appears.

Figure 4.2-1 USER ACCOUNTS Window



The **USER ACCOUNTS** window lists all accounts in the user account database. The data listed for each account entry is displayed under the following column headings:

*

A (add), D (delete), or M (modify) indicate pending changes made to the account.

LOGIN NAME

Name used at login.

USER ID

Number assigned to the user by the system.

DESCRIPTION

Description of the account.

To create a user account

NOTES ON USER ACCOUNTS

This section explains how to add a user account. However, adding a passive FTP user account requires additional steps. For instructions on adding a passive FTP user account, see the Help system.

When you de-install the DEBX COE, all user accounts are removed from the user accounts database. Therefore, when you install a new version of the DEBX COE (as described in [Section 7.4.6](#) of the *System Administrator's Guide for DOD E-Business Exchange System*), you must re-add all user accounts. Otherwise, you should simply verify that all user accounts are present.

1. Determine if a default role (i.e., Security Admin, System Admin, or DEBX Operator) will be assigned to the account, or if a new role should be created.

If necessary, create a new role for the account (as described in [Section 4.3](#)).

2. Log in as `root`.
3. In the **Console** window, enter `/usr/sbin/sam` to run the HP® System Administration Manager (SAM) and press [Enter]. The **System Administration Manager** window appears.
4. In the **SAM Areas** box, select **Accounts for Users and Groups**.

5. Select **Users**. The **Accounts for Users and Groups** window appears, listing all existing accounts.
6. From the **Actions** menu, select **Task Customization**.
7. Verify that the **Command to Run After Adding Users** field contains `/etc/FixAcct`. If it does not, enter `/etc/FixAcct` into this field.
8. Select **OK**. A **Note** window appears, confirming the configuration.
9. Select **OK**. The **Accounts for Users and Groups** window reappears.
10. From the **Actions** menu, select **Add**. The **Add a User Account** window appears.
11. Enter the following items:

In this field:	Enter:
Login Name	<login_name of user account>
Home Directory	/h/USERS/<login_name>/Scripts
Primary Group Name	hawk
Start-up Program	/usr/bin/csh

12. Select **OK**. The **Set User Password** window appears.

NOTE: If the system is running in trusted mode, it is not required to designate a password for the user at this time. Instead, a unique user identification number is assigned to the user. When the user initially logs into DEBX, the system prompts the user to change the password.

13. Enter a password for the user account and select **OK**.
14. Reenter the password and select **OK**. A **Note** window appears, confirming the addition of the user account.
15. Select **OK**. The **Accounts for Users and Groups** window reappears, displaying the newly added user account.
16. Repeat [Step 10](#) through [Step 15](#) for each user account you wish to add.
17. When finished adding user accounts, select **Exit** from the **File** menu. The **System Administration Manager** window appears.
18. From the **File** menu, select **Exit SAM**.

19. In the Console window, enter `exit`.
20. Log in as `secman`.
21. From the Accounts menu, select View User Accounts. The USER ACCOUNTS window appears, displaying the user accounts that were created using HP-SAM.
22. Select a user account and then click EDIT. The EDIT ACCOUNT window appears.

Figure 4.2-2 EDIT ACCOUNT Window

ACCOUNT GROUPS		ROLES	
<input type="checkbox"/>	root	<input checked="" type="checkbox"/>	SSO Default
<input checked="" type="checkbox"/>	Security Admin	<input checked="" type="checkbox"/>	SA Default
<input checked="" type="checkbox"/>	System Admin	<input checked="" type="checkbox"/>	DEBX Default
<input checked="" type="checkbox"/>	DEBX Operator		

23. The **DESCRIPTION** field defaults to the description entered in the `/etc/passwd` file for the user. If there is no description in the `/etc/passwd` file for this user, the field is blank. You may enter a short (up to 35 characters) description of the account in this field; however, these changes are not automatically saved to the `/etc/passwd` file. You must manually enter the description in the `/etc/passwd` file for your changes to take effect.
24. In the **ACCOUNT GROUPS** box, select one or more account groups for the user account. An account group defines general access to applications. The account groups are:
 - *root* – direct access to the UNIX system
 - *Security Admin* – access to the security applications
 - *System Admin* – access to the system administration applications
 - *DEBX Operator* – access to the user applications
25. From the **ROLES** box, select one or more roles for the user account. A role assigns specific functionality within an application. For instructions on either creating a new role or viewing the functionality assigned to an existing role, see [Section 4.3](#).
26. Click OK. The USER ACCOUNTS window reappears, displaying M in the * column for the account.

27. Repeat [Step 22](#) through [Step 26](#) for each new user account.
28. When finished editing user accounts, click OK in the USER ACCOUNTS window.

NOTE: You *must* click SAVE or OK in the USER ACCOUNTS window to accept any editing changes. If you click CANCEL, all changes made to the USER ACCOUNTS window will be discarded.

To delete a user account

NOTE: Default user accounts cannot be deleted.

1. Log in as `secman`.
2. From the Accounts menu, select View User Accounts. The USER ACCOUNTS window appears.
3. Select the user accounts to be removed and then click DELETE. The ANSWER PLEASE window appears, asking if you wish to mark the selected account(s) for deletion.
4. Select OK. In the USER ACCOUNTS window, a D appears in the * column for each selected account.
5. Select OK to close the USER ACCOUNTS window and delete the marked account(s).
6. From the System menu, select System Exit.
7. Log in as `root`.
8. In the Console window, enter `/usr/sbin/sam` to run HP SAM and press [Enter]. The System Administration Manager window appears.
9. In the SAM Areas box, select Accounts for Users and Groups.
10. In the SAM Areas box, select Users. The Accounts for Users and Groups window appears, listing all existing accounts.
11. Select the user account to be deleted and then select Remove from the Actions menu. The Remove a User window appears.
12. Select the Removed from All File Systems option and then select OK. A Confirmation window appears, asking if you wish to continue.

13. Select YES. A Note window appears, explaining that the system will remove the user account and any related files.
14. Select OK.

To retain a user account marked for deletion

Select UNDELETE from the pop-up menu for the USER ACCOUNTS window. The D in the * column for the entry will disappear, and the account will remain in the list.

To generate a printed report

In the USER ACCOUNTS window, click PRINT. For a detailed description of how to set up a printer, see the *System Administrator's Guide for DOD E-Business Exchange System*.

4.3 View Roles

The View Roles option enables you to view, create, or modify a role. A role specifies a user's access to menus and options. After you create the roles needed at your site, you may use the View User Accounts option (as described in [Section 4.2](#)) to assign each role to one or more user accounts.

A role definition includes:

- role name
- security level
- account group (DEBX Operator, System Admin, or Security Admin)
- access to the menus and options within the account group
- capability permissions

A role is also used to track login and logout events in the audit log. Multiple roles may be created for an account group, and multiple account groups and roles may be assigned to a user account. The current user's role will appear in the right corner of the DEBX main menu bar.

Three default roles delivered with the system provide access to all functions of the assigned account group:

- SSO Default
 - Security Admin account group
 - Access to all security application menus and options
 - Unclassified classification
- SA Default
 - System Admin account group
 - Access to all system administration menus and options
 - Unclassified classification
- DEBX Default
 - DEBX Operator account group
 - Access to all DEBX COE segments and DEBX application segment menus and options
 - Unclassified classification

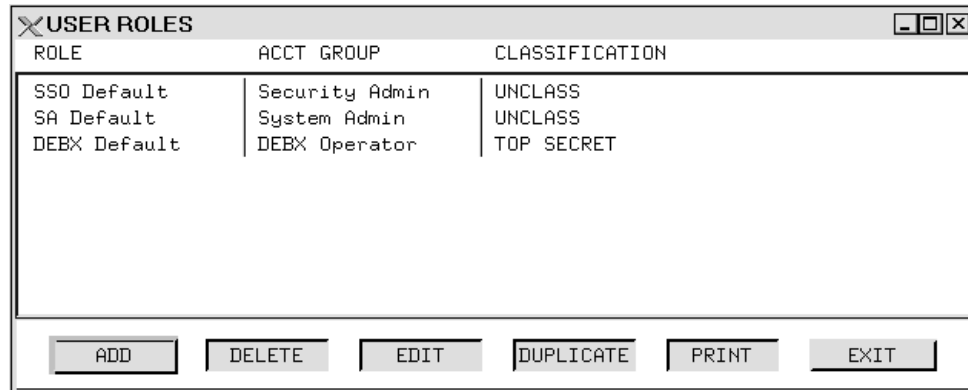
Using the View Roles option, you can do the following:

- [Access](#) the user roles database.
- [Create](#) a user role.
- [Delete](#) a user role.
- [Edit](#) a user role.
- [Duplicate](#) a user role.
- [Generate](#) a printed report.

To access the user roles database

From the Accounts menu, select View Roles. The USER ROLES window appears.

Figure 4.3-1 USER ROLES Window



ROLE	ACCT GROUP	CLASSIFICATION
SSO Default	Security Admin	UNCLASS
SA Default	System Admin	UNCLASS
DEBX Default	DEBX Operator	TOP SECRET

ADD DELETE EDIT DUPLICATE PRINT EXIT

Each entry in the USER ROLES window includes data under the following column headings:

ROLE

Name of the role.

ACCT GROUP

Account group associated with the role.

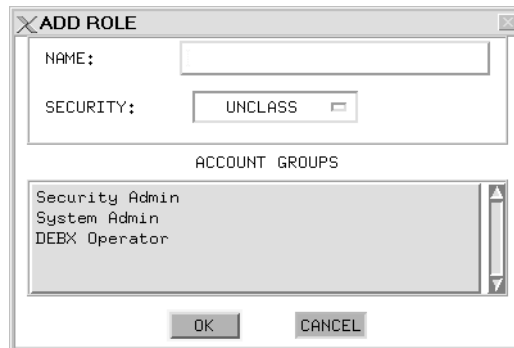
CLASSIFICATION

Security classification of the role.

To create a user role

1. In the USER ROLES window, click ADD. The ADD ROLE window appears.

Figure 4.3-2 ADD ROLE Window



The screenshot shows a dialog box titled "ADD ROLE". It has a standard Windows-style title bar with a close button. The dialog contains three labeled sections: "NAME:" followed by a text input field; "SECURITY:" followed by a dropdown menu currently showing "UNCLASS"; and "ACCOUNT GROUPS" followed by a list box containing three items: "Security Admin", "System Admin", and "DEBX Operator". At the bottom of the dialog are two buttons: "OK" and "CANCEL".

2. In the NAME field, enter a name for the role.
3. Click the list box in the SECURITY field to display a list of valid security classifications. Select a classification from the list.
4. From the ACCOUNT GROUPS box, select one account group for the role. An account group defines general access to applications. The account groups are:
 - *Security Admin* – access to the security applications
 - *System Admin* – access to the system administration applications
 - *DEBX Operator* – access to the user applications

Note that the root account group (which is used specifically to access UNIX system files) cannot be associated with a role and therefore is not listed in the ACCOUNT GROUPS box.

5. Click OK to accept the new role. The EDIT ROLE window ([Figure 4.3-3](#)) opens to allow you to define the role.

To delete a role

NOTE: Default roles and roles currently assigned to a user account cannot be deleted.

1. In the **USER ROLES** window, select one or more roles.
2. Click **DELETE**. A confirmation window appears to verify the deletion.
3. Click **YES** to confirm the deletion. The role is removed from the **USER ROLES** window and will not appear in the **ROLES** list in the **EDIT ACCOUNT** window ([Figure 4.2-2](#)).

To edit a role

Keep the following in mind when editing a role:

- Access to menus and functions can be expanded or reduced.
- When new segments are loaded, additional menus and options will be available. A role can be expanded to include the added functionality.
- When segments are removed, menus and options are automatically deleted from associated roles. However, user accounts assigned the roles will retain the previous role information. Open the **EDIT** window for each user account (see [Section 4.2](#) for instructions) and modify at least one field. The user account will then incorporate the revised role.

1. In the **USER ROLES** window, select a role and then click **EDIT**. The **EDIT ROLE** window appears.

Figure 4.3-3 *EDIT ROLE* Window

EDIT ROLE

ROLE HEADER

NAME: SSO Default

ACCT GROUP: Security Admin

SECURITY: TOP SECRET

PERMISSIONS

Accounts	ADEPRVX
Audit Status	E
Classification	E
Logs	DPV
Roles	ADEPRVX

A:Add D:Delete E:Edit
P:Print R:Restore V:Archive
X:Export

EDIT

MENU ACCESS

Sec Admin

EDIT

OK **CANCEL**

2. In the **ROLE HEADER** box, click the list box in the **SECURITY** field to display a list of valid security classifications. Select an entry from the list.
3. Use the **PERMISSIONS** box to define the specific functions available to each user assigned to the role.

Categories and functions that appear in the **PERMISSIONS** box depend on the account group selected for the role. Currently, categories and functions are not displayed for the DEBX Operator account group. A user assigned to this account group may access all menu options. Therefore, all categories and functions of the system will be provided. To prohibit the use of certain functions, menu option access can be restricted using the **MENU ACCESS** box (discussed in [Step 4](#)).

The remaining account groups with their categories and subset of functions are as follows:

Table 4.3-1 Security Administration Functions

Category	Add	Delete	Edit	Print	Restore	Archive	Export
Accounts	X	X	X	X	X	X	X
Audit Status			X				
Classification			X				
Logs		X		X		X	
Roles	X	X	X	X	X	X	X

Table 4.3-2 System Administration Functions

Category	Mount	Un-mount	NEWFS	Init Floppy	Mount New	Add	Delete	Edit
DiskManager	X	X	X	X	X			
EditHosts						X	X	X

- a. For the Security Admin and System Admin account groups only: In the **PERMISSIONS** box, select one category in the scroll list and then click **EDIT**. The **EDIT PERMISSIONS** window appears.

Figure 4.3-4 EDIT PERMISSIONS Window



- b. Select the checkboxes for functions that should be available to a user assigned this role. (All functions are off when a new role is created.)
 - For example, you could specify that a user can add, print, restore, archive, and export an account, but cannot delete or edit an account.
 - Only the functions that are applicable for the selected category are shown in the **EDIT PERMISSIONS** window.
- c. Click **OK** to accept the changes, or **CANCEL** to discard. Clicking either button closes the window.
- d. Repeat this process for other categories in the **PERMISSIONS** box.

4. Use the MENU ACCESS box to select the menus and options for the role, as follows:
 - a. In the MENU ACCESS box, select the name of the menu bar that appears in the window. The name of this menu bars depends on the account group you selected when you created the role (as described in [Step 4](#) of “*To create a user role.*”)
 - b. Click EDIT. The EDIT MENU ACCESS window appears, displaying a list of the menu options available for the menu bar.
 - c. Click the arrow left of the menu name to reveal a cascading list of options for that menu.
 - d. To enable or restrict access to any of the menus or options, toggle the checkbox adjacent to the name of the menu or option on or off. (All menus and options are on by default when a role is created.)
 - If a menu or option is on (shaded) it is available to a user assigned this role.
 - If a menu or option is off (blank) it will not appear on the menu bar or the pull-down menu for a user assigned this role.
 - e. Click OK to accept the changes.
 - f. Repeat this process for other menu bars in the scroll list.
5. In the EDIT ROLE window, click OK to accept the role.

To duplicate a role

1. From the USER ROLES window, select a role to duplicate.
2. Click DUPLICATE.
3. In the DUPLICATE ROLE window, enter a new role name.
4. Click OK to accept the name and close the window. The duplicate role is listed in the USER ROLES window. Use EDIT to make changes to the new role.

To generate a printed report

In the USER ROLES window, click PRINT. For a detailed description of how to set up a printer, see the *System Administrator’s Guide for DOD E-Business Exchange System*.

4.4 Archive Accts & Roles

The Archive Accts & Roles option enables you to archive user account and role information to tape.

From the Accounts menu, select Archive Accts & Roles. The ARCHIVE ACCTS & ROLES window appears.

Figure 4.4-1 ARCHIVE ACCTS & ROLES Window



To archive accounts and roles

1. Select Accounts or Roles, or both.
2. Click ARCHIVE (or click CANCEL to discontinue the archive process).
3. Insert a tape and click OK in the warning window. A confirmation window appears before proceeding with the archive process.
4. Click YES to continue with the archive, or NO to cancel the process.

NOTE: The archive process cannot be canceled after YES is selected.

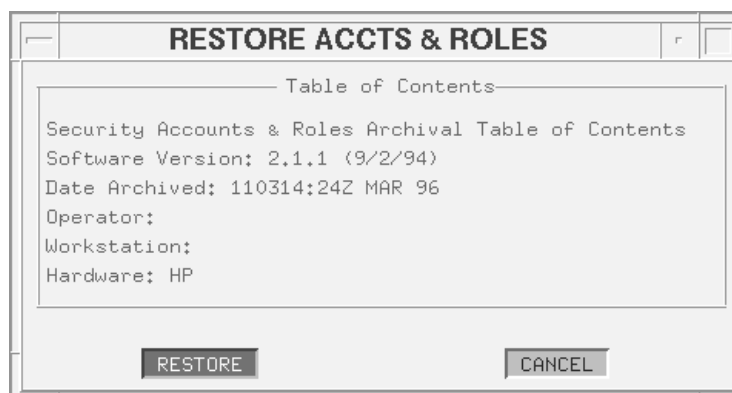
4.5 Restore Accts & Roles

The Restore Accts & Roles option enables you to restore all accounts and roles from tape to a workstation.

To restore accounts and roles

1. From the Accounts menu, select the Restore Accts & Roles option. A warning window appears.
2. Insert the tape and then click OK in the warning window. A confirmation window appears.
3. Click YES to continue or NO to cancel the restore process. If you click YES, the RESTORE ACCTS & ROLES window appears, displaying the tape's table of contents.

Figure 4.5-1 RESTORE ACCTS & ROLES Window



NOTE: If you click **RESTORE**, the system overwrites the current account and role information on the workstation with the information on the tape.

4. Click **RESTORE** to read the tape and overwrite the workstation's account and role information, or click **CANCEL** to cancel the restore process.

This page has been intentionally left blank.

Section 5

Help

The options on the **Help** menu enable you to view the online documentation for DEBX. |

The **Help** menu provides the following options:

Contents and Index

To view the online Help system, which provides step-by-step instructions for using DEBX. |

System Admin Guide

To view the online *System Administrator's Guide for DOD E-Business Exchange System*, which details the duties of the system administrator and describes how to install DEBX.

Security Mgr Guide

To view the online *Security Manager's Guide for DOD E-Business Exchange System*, which outlines the role of the security manager. |

This page has been intentionally left blank.

Security Manager's Guide for DEBX

Index

A

account

- archiving, [4-18](#)
- printing database, [4-3](#)
- restoring, [4-19](#), [4-19](#)
- user
 - accessing, [4-4](#)
 - caution, [4-8](#)
 - creating, [4-5](#)
 - default, [4-4](#)
 - deleting, [4-8](#)
 - printing, [4-9](#)
 - retaining deleted, [4-9](#)
- viewing database, [4-2](#)

account group

- DEBX operator, [4-7](#)
- definitions, [4-7](#)
- root, [4-7](#), [4-12](#)
- security admin, [4-7](#)
- selecting, [4-7](#)
- system admin, [4-7](#)

account groups, user, [4-15](#)

accounts menu, overview of, [4-1](#)

alert, [3-6](#)

alert log

- archiving, [3-7](#)
- printing, [3-7](#)
- purging, [3-8](#)
- viewing, [3-6](#)

archive

- alert log, [3-7](#)
- caution, [3-9](#), [4-18](#)
- user account, [4-18](#)
- user role, [4-18](#)

archive accts & roles option, [4-18](#)

archive logs option, [3-9](#)

audit

- information, archiving to tape, [3-7](#)
- information, purging from log, [3-8](#)

audit event, [3-4](#)

audit log, [3-4](#)

- archiving, [3-5](#)
- printing, [3-5](#)
- purging, [3-5](#)
- viewing, [3-4](#)

audit status option, [3-2](#)

D

database, system account

- overview of, [4-2](#)
- printing from, [4-3](#)
- viewing, [4-2](#)

DEBX default role, [1-2](#), [4-10](#)

DEBX operator account group, [4-7](#)

deleting, user role, [4-13](#)

document, online, [1-1](#)

E

editing, user role, [4-13](#)

event, audit, [3-4](#)

exiting system, [2-3](#)

F

font size, setting, [2-2](#)

L

log

alert

- archiving, [3-7](#)
- printing, [3-7](#)
- purging, [3-8](#)
- viewing, [3-6](#)

archiving, [3-9](#)

audit

- archiving, [3-5](#)
- printing, [3-5](#)
- purging, [3-5](#)
- viewing, [3-4](#)

security, [3-2](#)

size of, [3-3](#)

sorting, [3-5](#)

M

menu

setting font size, [2-2](#)menu, using, [1-2](#)misc menu, overview of, [5-1](#)**P**permissions, setting user, [4-14](#)

printing

alert log, [3-7](#)system account report, [4-3](#)user role report, [4-17](#)**R**

restore

caution, [4-19](#)user account, [4-19](#)user role, [4-19](#)restore accts & roles option, [4-19](#)role, [4-10](#)archiving, [4-18](#), [4-18](#)assigning, [4-7](#)creating, [4-12](#)database, accessing, [4-11](#)database, printing, [4-17](#)DEBX default, [4-10](#)default, [4-10](#)definition, [4-10](#)deleting, [4-13](#)duplicating, [4-17](#)editing, [4-13](#)permissions, [4-14](#)restoring, [4-19](#), [4-19](#)SA default, [4-10](#)SSO default, [4-10](#)use of, [4-10](#)role box, using, [1-2](#)root account group, [4-7](#), [4-12](#)root user account, [4-4](#)**S**SA default role, [4-10](#)SAM, [4-5](#)secman user account, [4-4](#)security admin account group, [4-7](#)

security alert log

archiving, [3-7](#)printing, [3-7](#)viewing, [3-6](#)security alert log option, [3-6](#)security log, [3-2](#)security manager, definition, [1-1](#)security menu, overview of, [3-1](#)set menu font option, [2-2](#)SSO default role, [4-10](#)sysadmin user account, [4-4](#)

system account

overview of, [4-2](#)printing, [4-3](#)restoring, [4-19](#)viewing, [4-2](#)system admin account group, [4-7](#)System Administration Manager, *see* SAMsystem exit option, [2-3](#)system menu, overview of, [2-1](#)**U**

user account

accessing, [4-4](#)archiving, [4-18](#)caution, [4-8](#)creating, [4-5](#)default, [4-4](#), [4-4](#)deleting, [4-8](#)overview of, [4-4](#)printing, [4-9](#)restoring, [4-19](#), [4-19](#)retaining deleted, [4-9](#)root, [4-4](#)secman, [4-4](#)sysadmin, [4-4](#)user account groups, [4-15](#)

user role

archiving, [4-18](#), [4-18](#)assigning, [4-7](#)creating, [4-12](#)database, accessing, [4-11](#)database, printing, [4-17](#)DEBX default, [4-10](#)default, [4-10](#)definition, [4-10](#)deleting, [4-13](#)duplicating, [4-17](#)editing, [4-13](#)overview of, [4-10](#)permissions, [4-14](#)restoring, [4-19](#), [4-19](#)SA default, [4-10](#)SSO default, [4-10](#)use of, [4-10](#)**V**view roles option, [4-10](#)view system accounts option, [4-2](#)view user accounts option, [4-4](#), [4-4](#)

DEBX

Document Comment Form

We would like to know your comments and suggestions regarding this document. With your help, we will be able to make improvements to this and other DEBX documents in the future.

Please rate each of the following items by circling a response:

	POOR	FAIR	GOOD	VERY GOOD	EXCELLENT
1) Helpfulness	1	2	3	4	5
2) Accuracy	1	2	3	4	5
3) Readability	1	2	3	4	5
4) Organization	1	2	3	4	5
5) Easy to Understand	1	2	3	4	5

Please check your response to each of the following items:

- | | | |
|--|------------------------------|-----------------------------|
| 6) Does the document contain enough figures/illustrations? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 7) Is the level of detail adequate? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |
| 8) Does the document meet your needs as a reference guide? | <input type="checkbox"/> Yes | <input type="checkbox"/> No |

Please respond to each of the following questions:

- 9) What is missing from this document?

- 10) What do you like about this document?

- 11) What do you dislike about this document?

Please enter any additional comments or suggestions in the space below.

Date: _____
Name: _____
Position/Title: _____
Address: _____
City/State: _____

This form is ready to be mailed to the address printed on the reverse. Just fold and seal this form with tape or staples, affix a stamp, and mail it. Or, if you prefer, place this form in an envelope and address the envelope for mailing.

FOLD

Place
Stamp
Here

Documentation Manager
Inter-National Research Institute, Inc.
12350 Jefferson Avenue, Suite 400
Newport News, VA 23602

FOLD